UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/630,076	07/30/2003	Robert A. Koontz	D/A3245	6785

25453 7590 03/21/2007
PATENT DOCUMENTATION CENTER
XEROX CORPORATION
100 CLINTON AVE., SOUTH, XEROX SQUARE, 20TH FLOOR
ROCHESTER, NY 14644

EXAMINER	
HO, THOMAS M	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/630,076	KOONTZ ET AL.	
	Examiner	Art Unit	
	Thomas M. Ho	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☒ ~~Claim(s) 11-14 is/are objected~~ to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/12/06, 7/20/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-19 are pending.

Claim Objections

2. Claim 1 ~~1-14 are objected to as being~~ dependent upon a rejected base claim, but would be allowable if rewritten ~~in~~ independent form including all of the limitations ~~of the~~ base claim and any intervening claims.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-19 ~~1-10, 15-19~~ are rejected under 35 U.S.C. 103(a) as being unpatentable over Reardon, US patent 6212635.

Reardon discloses a method for managing machine operation options and configuration comprising:

- Providing a master key software operation key separable from the machine, where the master key software operation key is the MASTER TOKEN. (Column 8, lines 38-67) & (Column 9, line 65 – Column 11, line 15)
- Providing a subsequently installed software operation key separable from the machine, the subsequently installed software operation key further comprising a memory, with a programmable serial region and an option code, where the subsequently installed software operation keys are the tokens for individual users. (Column 11, line 15 – Column 12, line 10)
- Placing the subsequently installed software operation key into the machine, where the subsequently installed software operation keys are inserted into the token reader. (Figure 1, Items 14, 16)
- Reading the programmable serial region of the memory and if found blank, initializing with a machine identification number, where the programmable serial region of the memory is initialized with manufacturer security, key, and identification information. (Column 9, lines 54-67)
- Reading the memory and installing the option code into the master key software operation key, where the option code is the specific rights and restrictions of each user stored on the token. (Column 11, lines 20-30)
- Operating the machine in accordance with the option code in the master key software operation key, where the option codes are the rights with which a user may access the data and where the machine is run in accordance with those access rules and rights. (Column 11, lines 30-45)

Reardon fails to explicitly disclose comparing the content of the programmable serial region if not blank with the machine identification number;

However, those of ordinary skill in the art recognize that the process of authenticating commonly necessitates a step of comparing the content of a token, key, or certificate with a reference value. Authentication is the process of verifying the identity of an entity. Usually an entity seeking to be authenticated will provide a value or ID, which will be matched against a database of record to determine if validity of the identity is true, and if so, to authorize the user.

Examples of authentication that compare values to validate identity include:

USPN: 5928363

(37) The server and application will resume the session with the client only if the authenticating token compares equal to a client on the server-stored authorized list. In the event of noncomparison, the server and application will communicate a retry request to the client. This process is designed to be repeated a predetermined number of times.

USPN: US-PAT-NO: 5649185

2. The method of claim 1, further including:

the processor generating and retaining in the client store the new authenticating token for the client process before providing the first, second, and third messages;

the processor, the library server, and the associated image server including a copy of the new authenticating token in the first, second, and third messages, respectively;

the processor comparing the copy of the new authenticating token in the third message with the new authenticating token retained at the processor in

the client store before the transferring step; and

the processor continuing execution of the transferring step if the copy of the new authenticating token in the third message matches the new authenticating token retained in the client store; otherwise,

US-PAT-NO: 6236981

(15) e) at the payment server, authenticating the token by comparing the value of the random number of the token from the merchant platform and a value derived from a corresponding position in the stored sequence of random numbers; and

USPN 5103081:

21. A method for authenticating a gaming chip as recited in claim 17, wherein there are a plurality of said characteristics, wherein one of said characteristics identifies a serial number for said chip, and wherein said step of comparing includes comparing said serial number with a list of acceptable serial numbers to determine whether said chip is accepted or rejected.

USPN: 6795703

(33) Subsequently to step S12 or S14, the service provider consults the customer database, using the given information as search keywords, thereby validating the application (step S15). That is, the proposed system first searches the customer database for a record corresponding to the requesting customer's phone number. In the case of the application method (a), the system then performs user authentication by comparing the serial number and the customer's call forwarding password with the database record.

It would have been obvious to one of ordinary skill in the art at the time of invention to compare the content of the programmable serial region if not blank with the machine identification number in order to authenticate the master token and the user tokens to determine if access should be granted.

In reference to claim 2:

Reardon fails to explicitly disclose the embodiment wherein the machine is a printing apparatus. However Reardon does disclose that the purpose of the token reader and the security gateway is to regulate access to a computer system or peripheral devices such as that shown in Figure 1, Item 20.

The examiner takes official notice that a printer was a common peripheral device to those of ordinary skill in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art to regulate access to a machine or digital device where the machine was a printer in order to prevent access by unauthorized users to printers on a network.

In reference to claim 3:

Reardon fails to explicitly disclose the embodiment wherein the machine is a multi-function office device.

However Reardon does disclose that the purpose of the token reader and the security gateway is to regulate access to a computer system or peripheral devices such as that shown in Figure 1, Item 20.

The examiner takes official notice that a multi-function office device was a common peripheral device to those of ordinary skill in the art at the time of invention. For example: scanners that double up as fax devices, or printers/scanner/fax machines are frequently employed by companies as a convenience and cost cutting measure.

It would have been obvious to one of ordinary skill in the art to regulate access to a machine or digital device where the machine was a multi-function office device in order to regulate access to authorized users on a network.

In reference to claim 4:

Reardon (Column 11, line 65 – Column 12, line 10) discloses the method of claim 1 wherein the memory is a nonvolatile type of memory.

In reference to claim 5:

Reardon discloses method of claim 1 wherein the software operation key is a CRUM.

Where those of ordinary skill in the art recognize that a CRUM is an electronic device that includes nonvolatile memory that is a replaceable module.

US patent 6351621 paragraph (4) illuminates :

(4) In the office equipment industry, the concept of the "customer replaceable unit monitor," or CRUM, is well known. A CRUM is generally an electronic device which is permanently associated with a replaceable module which may be installed in a printer or copier. Typically, the CRUM includes a non-volatile memory, such as in the form of an EEPROM, which retains data relevant to the function and performance of the module...

In reference to claim 6:

Reardon fails to explicitly state the method of claim 1 wherein the machine identification number is the machine serial number.

However, Reardon discloses that the information stored on the master key software operation key includes passwords, certificates of authority, and security parameters.

Reardon later states in paragraph 96 that the machine serial number is an example of security data.

> (96) The key to this technique is the ability to confirm that a communicating computer is indeed under the supervision of an authentic security gateway. This can be accomplished by the manufacturer embedding in each device a "public key" that is common to all of the security gateways in that line of products. In this example, it will be assumed that SG.0B is used, although there could be a different key used for this specific purpose. At the start of a CERTIFIED TRANSACTION, the security gateway would encrypt a SELF-IDENTIFYING MESSAGE, including, for example, its own serial number, the version of the GATEWAY PROGRAM and SHELL in use, and a copy of SG.1B, using SG.0B. This SELF-IDENTIFYING MESSAGE is sent over the Internet to the manufacturer using a proprietary protocol for added security and verification of identity. The manufacturer's host site uses SG.0R to decrypt the package, thereby confirming that the SELF-IDENTIFYING MESSAGE must have been encrypted by an authentic security gateway since only security gateways manufactured by the company have access to the SG.0B. The authenticity of the security gateway can be further confirmed by including in the SELF-IDENTIFYING MESSAGE, other security gateway embedded data, such as a serial number, and the fact that the proprietary communications protocol was properly used.

It would have been obvious then to include the serial number among the certificates of authority or security parameters as additional security data that is relevant to Reardon's authentication process in order to provide an additional unique means of identifying information.

Claim 7 is rejected for the same reasons as claim 2.

Claim 8 is rejected for the same reasons as claim 4.

In reference to claim 9:

Reardon paragraph (0011) discloses the printing machine of claim 8 wherein the non-volatile memory is an EEPROM.

(11) Non-volatile memory: Memory locations that preserve their stored information even when power has been removed from the memory banks and/or computer system. Typical examples of non-volatile memory include ROM, EEPROM, Flash memory devices, and magnetic storage media.

KAMBIZ ZAND
PRIMARY EXAMINER

Claim 10 is rejected for the same reasons as claim 5.

Claim 11-14 are rejected since a recitation directed to the manner in which a claimed apparatus, system or Method to be used does not distinguish the claims from the Prior art if the prior art has the capability to do so Perform see MPEP 2114 and Ex Parte Masham 2 USPQ2d 1647 (1987)

In reference to claim 15:

Reardon fails to disclose the printing machine of claim 7 wherein the option code directs the printing machine to configure for job based accounting.

The Examiner takes official notice that storing an option code to direct the printer machine to configure for job based accounting was well known at the time of invention. Richards et al. USPN 6351621 discusses the prior art of CRUMs (Column 4, lines 10-45) where the CRUM serves as an "odometer" to count the number of printer jobs.

In reference to claim 16:

Reardon discloses a method for managing machine operation options and configuration comprising:

- Providing a master key software operation key separable from the machine the master software operation key further comprising a first memory, with a first programmable serial region and a first option code, where the master key software operation key is the MASTER TOKEN. (Column 8, lines 38-67) & (Column 9, line 65 – Column 11, line 15)
- Providing a subsequently installed software operation key separable from the machine, the subsequently installed software operation key further comprising a second memory, with a second programmable serial region and a second option code, where the subsequently installed software operation keys are the tokens for individual users. (Column 11, line 15 – Column 12, line 10)
- Placing the master key software operation key into the machine, where the subsequently installed software operation keys are inserted into the token reader. (Figure 1, Items 14, 16)
- Reading the first programmable serial region of the first memory and if found blank, initializing with a machine identification number, where the programmable serial region of the memory is initialized with manufacturer security, key, and identification information. (Column 9, lines 54-67)

- Placing the subsequently installed software operation key into the machine; (Figure 1, Items 14, 16)
- Reading the second programmable serial region of the second memory and if found blank, initializing with the machine identification number. (Column 11, lines 15-33)
- Reading the memory and installing the option code into the master key software operation key, where the option code is the specific rights and restrictions of each user stored on the token. (Column 11, lines 20-30)
- Operating the machine in accordance with the first option code and the second option code in the master key software operation key, where the option codes are the rights with which a user may access the data and where the machine is run in accordance with those access rules and rights. (Column 11, lines 30-45)

Reardon fails to explicitly disclose comparing the content of the programmable serial regions of the tokens with the machine identification number;

However, those of ordinary skill in the art recognize that the process of authenticating commonly necessitates a step of comparing the content of a token, key, or certificate with a reference value. Authentication is the process of verifying the identity of an entity. Usually an entity seeking to be authenticated will provide a value or ID, which will be matched against a database of record to determine if validity of the identity is true, and if so, to authorize the user.

Examples of authentication that compare values to validate identity include:

USPN: 5928363

(37) The server and application will resume the session with the client only if the authenticating token compares equal to a client on the server-stored authorized list. In the event of noncomparison, the server and application will communicate a retry request to the client. This process is designed to be repeated a predetermined number of times.

USPN: US-PAT-NO: 5649185

2. The method of claim 1, further including:

the processor generating and retaining in the client store the new authenticating token for the client process before providing the first, second, and third messages;

the processor, the library server, and the associated image server including a copy of the new authenticating token in the first, second, and third messages, respectively;

the processor comparing the copy of the new authenticating token in the third message with the new authenticating token retained at the processor in the client store before the transferring step; and

the processor continuing execution of the transferring step if the copy of the new authenticating token in the third message matches the new authenticating token retained in the client store; otherwise,

US-PAT-NO: 6236981

(15) e) at the payment server, authenticating the token by comparing the value of the random number of the token from the merchant platform and a value derived from a corresponding position in the stored sequence of random numbers; and

USPN 5103081:

21. A method for authenticating a gaming chip as recited in claim 17, wherein there are a plurality of said characteristics, wherein one of said characteristics identifies a serial number for said chip, and wherein said step

of comparing includes comparing said serial number with a list of acceptable serial numbers to determine whether said chip is accepted or rejected.

USPN: 6795703
(33) Subsequently to step S12 or S14, the service provider consults the customer database, using the given information as search keywords, thereby validating the application (step S15). That is, the proposed system first searches the customer database for a record corresponding to the requesting customer's phone number. In the case of the application method (a), the system then performs user authentication by comparing the serial number and the customer's call forwarding password with the database record.

It would have been obvious to one of ordinary skill in the art at the time of invention to compare the content of the programmable serial region if not blank with the machine identification number in order to authenticate the master token and the user tokens to determine if access should be granted.

Claim 17 is rejected for the same reasons as claim 9.

Claim 18 is rejected for the same reasons as claim 5.

Claim 19 is rejected for the same reasons as claim 6.

Conclusion

10. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Gilberto Barron can be reached on **(571)272-3799.**

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 571-273-8300
Customer Service Representative	Telephone: 571-272-2100	Fax: 571-273-8300

TMH

November 25th, 2005